

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28

2

3
4

7
8
9
10
11

12

13
14
15
16
17

18

19
20
21
22
23
24
25
26
27
28

1 and decryption is as long as the message, and if the key is used
2 only once, the encryption method is referred to as a One-Time Pad
3 (OTP) encryption method. If the key is shorter than the
4 plaintext message, such that the key, or a derivative of the key,
5 must be used two or more times, the encryption method is referred
6 to as a "repeating key" encryption method. Prior to the
7 development of computers that included dense, efficient, and re-
8 writable data storage devices, the use of the OTP encryption
9 method for any but the shortest of messages was extremely
10 difficult and time consuming, due to the sheer size and volume of
11 the necessary encryption keys needed. For example, for a person
12 to encrypt a one megabyte computer file, the OTP cipher requires
13 a one megabyte encryption key that cannot be reused. This system
14 requirement made the implementation of an OTP cipher system very
15 difficult and nearly impractical, prior to the advent of
16 computers. This caused the OTP cipher to be relegated to only
17 the most critical situations involving very small messages.
18 Therefore, almost no development has occurred on the use and
19 deployment of the One-Time Pad. Repeating keys have been favored
20 over One-Time Pad keys because they are much smaller (typically
21 hundreds or thousands of times smaller) and can be reused.

22 A popular repeating key method known as public key
23 encryption uses different but related public and private keys for
24 encryption and decryption. With the development of computers
25

1 that include fast, easy to use, and removable data storage media
2 (like flash RAM memory devices using universal serial bus (USB)
3 interfaces capable of secure storage and management of the very
4 large encryption keys needed for practical OTP deployment), the
5 use of OTP encryption for data communication and storage has
6 become practical. Additionally, with the recent increases in
7 computer speed and memory size, repeating key encryption methods
8 previously thought to provide adequate security have been broken,
9 and are being broken at an increasing rate. Given a large enough
10 sample of encrypted messages and a fast enough computer with a
11 large enough memory, any repeating key encryption scheme can be
12 broken. The only known encryption method that is provably
13 unbreakable and immune to these advances in computer processing
14 power and speed is the One-Time Pad cipher.
15

16
17 One of the primary challenges to encrypted communications is
18 the need to distribute, update, and replace encryption keys.
19 Although this need applies to all cipher systems, it is
20 especially acute with the One-Time Pad cipher. Prior to this
21 invention, there was no secure way to distribute, update, and
22 replace keys by any means other than to physically deliver said
23 keys to each participant in the communications channel. In the
24 present invention, OTP and other encryption keys can be
25 distributed in a secure manner even over insecure electronic
26 means like the Internet, rather than through physical
27
28

1 distribution methods. Thus, the present invention geometrically
2 increases the use, scalability, encryption volume, surge
3 capabilities, and efficiency of the OTP and other cipher systems.

4 Disclosure of Invention

5 Methods, computer-readable media, and apparatus for securely
6 distributing a cryptographic key (C) from a first party(s) to a
7 second party(s). A method embodiment of the present invention
8 comprises the steps of combining (steps 1 and 2) the
9 cryptographic key (C) with a transport key (T) to form a key set;
10 encrypting (step 7) the key set to form an encrypted key set;
11 distributing (step 8) the encrypted key set across a medium (3);
12 and decrypting (step 9) the encrypted key set to reconstitute the
13 cryptographic key (C) and the transport key (T).
14

15 Brief Description of the Drawing

16 These and other more detailed and specific objects and
17 features of the present invention are more fully disclosed in the
18 following specification, reference being had to the accompanying
19 drawing, in which:
20

21 Figure 1 is a state diagram illustrating operation of the
22 present invention, with method steps shown as lines connecting
23 the states.
24

25 Detailed Description of the Preferred Embodiments

26 As used throughout this specification and claims, the
27 following terms have the following meanings:
28

1 "One-Time Pad Cipher" (OTP) is a unique cipher, or class of
2 ciphers, that uses a key as long as the original plaintext
3 message. The key is consumed during an exclusive OR (XOR)
4 encryption process and must never be reused. Because the key is
5 a consumable, it must be replaced when it reaches or nears the
6 end of its volume.
7

8 "Key" is any sequence of symbols of any length that is used
9 to encrypt and/or decrypt information in any form.

10 "Compression" is an algorithm or the product of an algorithm
11 used for the reduction of the volume of binary data.

12 "Key folding" is a process of compressing a key so that the
13 total volume, represented by the number of bits or bytes in the
14 key, is one half of the original volume of the key before
15 compression.
16

17 "LSB" means "least significant bit" or "least significant
18 bits", i.e., the rightmost bit or bits of an ordered sequence of
19 bits.
20

21 "MSB" means "most significant bit" or "most significant
22 bits", i.e., the leftmost bit or bits of an ordered sequence of
23 bits.

24 The invention will be illustrated for a computer system
25 having words that are 8 bits (one byte) long. In other
26 embodiments, the word length in bits is any power of two, i.e.,
27 16 bits, 32 bits, 64 bits, etc. The invention is illustrated
28

1 primarily with respect to a One-Time Pad cipher system. However,
2 the method can be used to distribute any type of cryptographic
3 key, such as a private (secret) key in a public key cryptosystem,
4 or a symmetric key in a symmetric cryptosystem such as RC4. The
5 illustrated method has 10 steps, and can be executed an
6 arbitrarily large number of iterations (assuming that no key is
7 lost, stolen, or corrupted), even when the keys C being
8 distributed are OTP keys, when the compression performed in step
9 six is 50% compression (key folding) or greater than 50%
10 compression. Two iterations of the method, plus an
11 initialization, are illustrated in Figure 1. For each successive
12 iteration, the subscripts on all the keys are incremented by one,
13 as can be seen by examining Figure 1.
14

15 In the example illustrated in Figure 1, the communications
16 keys C each have a volume of 5 (arbitrary) units, and the
17 transport keys T each have a volume of 10 units, i.e., 50%
18 compression is performed at step 6. An exception to the general
19 rule is that the first communications key C₀ does not have to
20 have a volume of 10 units, and in this case is shown as having 50
21 units.
22

23 In Figure 1, key sizes are written below the capital letters
24 designating the key types within the state boxes. Physical
25 entities are enclosed within boxes, and method steps are
26 identified on the lines connecting the boxes. Items to the left
27
28

1 of the dashed vertical line passing through secure distribution
2 path 2 and network 3 are under control of party A, and items to
3 the right of said line are under the control of party B. Party A
4 and party B can be humans or computers. Party A and party B wish
5 to communicate with each other in a secure manner. Party A can
6 be a key distribution center, in which case party A distributes
7 communications keys C to at least two (and possibly many) parties
8 including party B.
9

10 The boxes and lines connecting boxes that are illustrated in
11 Figure 1 can be implemented using software, firmware, hardware,
12 or any combination thereof, e.g., one or more application
13 specific integrated circuits (ASICs) can be used. The method
14 steps can be embodied in software resident on any computer-
15 readable medium or media, such as a hard disk, floppy disk, CD,
16 DVD, etc. For example, one computer-readable medium may contain
17 software for executing the steps performed by party A, and a
18 second computer-readable medium may contain software for
19 executing the steps performed by party B.
20

21 True Random Number Generator (TRNG) 1 is a cryptographically
22 approved non-deterministic random number generator, i.e., one
23 having no repeat period and an output rated for unbreakable
24 cryptography. An example of TRNG 1 is Model SG100 made by
25 Protego of Sweden. Secure distribution path 2 can comprise a
26 trusted courier, a face-to-face meeting between party A and party
27
28

1 B, biometric verification, or any other means deemed by party A
2 and party B to be secure enough for the communications that the
3 two parties wish to undertake. Network 3 can comprise any
4 electronic or non-electronic network or signal path, such as the
5 public switched telephone network (PSTN), a computer network, a
6 wired or wireless LAN (Local Area Network), a wired or wireless
7 WAN (Wide Area Network), a terrestrial microwave link, a
8 satellite communications network, a telegraph over which the
9 parties communicate using Morse code, a semaphore signaling
10 system, or any combination of any of the above. Network 3 may
11 comprise a secure network or an inherently insecure network such
12 as the Internet.
13

14 Note that many of the below-described method steps appear at
15 several places in Figure 1.
16

17 In step 1, a transport key T is created. For the special
18 case in which the compression method used in step 6 is key
19 folding using bit swapping, T is created by using TRNG 1 to
20 create a random sequence of bytes from any subset of bytes in
21 which the first four MSB in each byte are identical. One example
22 of a suitable range of bytes satisfying this criterion consists
23 of those 16 consecutive bytes from the ASCII character set 64
24 (decimal) through 79 (decimal). This corresponds to the ASCII
25 characters @ through O. This set of 16 bytes is illustrated in
26 Table 1 as follows:
27
28

ASCII	Decimal	Binary
@	64	0100 0000
A	65	0100 0001
B	66	0100 0010
C	67	0100 0011
D	68	0100 0100
E	69	0100 0101
F	70	0100 0110
G	71	0100 0111
H	72	0100 1000
I	73	0100 1001
J	74	0100 1010
K	75	0100 1011
L	76	0100 1100
M	77	0100 1101
N	78	0100 1110
O	79	0100 1111

TABLE 1

Any subrange within the ASCII character set can be used, as long as the four MSB in the ASCII character set are identical. Since the ASCII character set is sequentially coded, there are 16 sequential subsets of characters within the full (for an 8-bit word) range 0 (decimal) through 255 (decimal) that have the same four MSB. Randomness sufficient for cryptography is not affected by using an ASCII subset any more than if the transport key T consisted solely of 1's and 0's, as long as the output of TRNG 1 is rated as being sufficient for unbreakable cryptography.

The creation of such a transport key T can be achieved by using a table lookup (e.g., a MIME type of table lookup), mathematical formula, or any other process to convert a random binary string or random byte sequence into a random byte sequence of 16 serial ASCII values having uniform MSB. One example of such a process is an expansion by a factor of two of a key

1 randomly generated by TRNG 1 by means of concatenating a common
2 MSB sequence at uniform four bit intervals throughout the length
3 of the key.

4 When OTP encryption is used in step 7, as it must be when
5 the communications keys C being distributed are OTP keys, the
6 volume (size) of the transport key T must be greater than or
7 equal to the combined sizes of the communications key C to be
8 distributed in the next iteration plus the size of the compressed
9 transport key FT to be used in the next iteration. Thus, the
10 size of T_0 must be greater than or equal to the combined sizes of
11 C_1 plus FT_1 ; the size of T_1 must be greater than or equal to the
12 combined sizes of C_2 plus FT_2 ; etc.

13 Step 1 is one of the few steps that is performed during the
14 initialization, as can be seen by examining Figure 1. During
15 said initialization, the initial transport key T_0 is created in
16 step 1, then distributed from party A to party B via secure
17 distribution path 2 in a special step 4 that is performed only
18 during initialization. In an alternative embodiment (not
19 illustrated), T_0 can be generated by party B and then distributed
20 to party A across secure distribution path 2.

21 Step 2 is the creation of a communications key C. C is
22 created by tasking TRNG 1 to create a random sequence from the
23 full range of the ASCII character set 0 (decimal) through 255
24 (decimal). Step 2 is another one of the few steps that is
25
26
27
28

1 performed during the initialization. The initial communications
2 key C_0 created during initialization can be any size, as long as
3 C_0 is larger than the conversion key K (see step 3 below). C_0
4 need not be created in proportion relative to any transport key,
5 because the main purpose of C_0 is to generate K . In one
6 embodiment (not illustrated) C_0 is sent from party A to party B
7 via secure distribution path 2, and is subsequently used by party
8 B for use as a cryptographic key in encrypting and decrypting
9 messages sent between party B and other parties, such as party A.
10 In this embodiment, the only C that needs to be distributed from
11 party A to party B by secure means is C_0 -- all the subsequent
12 C 's can be distributed over network 3, which can be insecure.

13
14 In the working iterations (iterations subsequent to the
15 initialization), a new communications key C replaces a previous
16 communications key C when the previous communications key C
17 reaches or nears the end of its useful life. Thus, C_1 replaces
18 C_0 , C_2 replaces C_1 , etc. Each communications key C is created by
19 tasking TRNG 1 to create a random sequence from the full range of
20 the ASCII character set 0 (decimal) through 255 (decimal). The
21 method can be repeatable an arbitrarily large number of
22 iterations, even in an OTP cipher system. In this case, C_1 has a
23 volume 50% of the volume of the initially distributed transport
24 key T_0 , as illustrated in Figure 1.
25
26
27
28

1 Step 3 is the creation of a conversion key K. In the method
2 illustrated in Figure 1, step 3 is performed just during
3 initialization. In an alternative embodiment, step 3 is
4 performed during each iteration of the method, to enhance
5 security. In that case, K as it appears on Figure 1 can be
6 replaced by K_0 , K_1 , K_2 , etc. In another alternative embodiment, K
7 can be regenerated upon the occurrence of a preselected event,
8 e.g., the expiration of a preselected period of time. In yet
9 another alternative embodiment, K can be regenerated when it
10 expires or is about to expire. For example, in the embodiment
11 illustrated in Figure 1, K has a size of 30 and each T has a size
12 of 10. In this case, K may be used in the XORing process of step
13 5 to convert three different T's, after which K is regenerated.

14
15
16 In embodiments where K is generated in a numbered iteration,
17 and not just during initialization, K can be encrypted and sent
18 across network 3 from party A to party B for subsequent use by
19 party B. Alternatively, party B can generate K from its
20 corresponding C assuming that party B has knowledge as to how
21 party A generated K from C. This knowledge (as well as other
22 items of knowledge, such as the encryption algorithm used in step
23 7, the folding algorithm used in step 6, and the folding range
24 used in step 6) can be sent from party A to party B by secure
25 means prior to execution of the method iterations.
26
27
28

1 In one embodiment, K comprises the removed bytes that are
2 created by removing a continuous sequence of bytes from
3 communications key C. In this scenario, K typically has a size
4 between 100KB and 1MB. This implies that the size of the
5 communications key C from which K is extracted should be
6 considerably greater than 1MB, e.g., at least 20MB. Since the
7 sequence of bytes that is removed from C is continuous, the bytes
8 in K exhibit the same cryptographically approved qualities of C,
9 and are likewise from the range of the full ASCII character set 0
10 (decimal) through 255 (decimal).
11

12 In an alternative embodiment, K is generated by TRNG 1 and
13 comprises a random sequence from the full range of the ASCII
14 character set 0 (decimal) through 255 (decimal).
15

16 A given K can be smaller than its corresponding T, e.g., K_0
17 can be smaller than T_0 , in which case K is a repeating key.

18 Step 4 is performed only during initialization, as described
19 previously. At step 4, K and T_0 are distributed from party A to
20 party B across secure distribution path 2.

21 Step 5 is the conversion of a transport key T into a key
22 whose bytes are from the full range of ASCII values, without
23 compromising the random properties of the transport key T. As
24 stated earlier, a new K may be generated during each iteration,
25 whether by carving K out of C or by tasking TRNG 1 to create K.
26 In this case, step 5 is also performed once per iteration.
27
28

1 The conversion of T is accomplished by exclusive OR-ing
2 (XORing) T with the corresponding (by subscript, in embodiments
3 where there is more than one K) conversion key K. As stated
4 previously, K can be a repeating key; if K is smaller than T, K
5 can be reused until all the bits of T have been XORed. This
6 XORing is done so that the encryption step (step 7 below) is
7 performed on like character sets, thereby preserving the
8 randomness of the ciphertext.
9

10 Step 6 comprises compressing the transport key T. If it is
11 desired for the method to be continuable indefinitely in certain
12 cipher systems including an OTP cipher system, the compression
13 must entail key folding (i.e., compression by 50%), or
14 compression by more than 50%. For distribution of certain types
15 of non-OTP keys, step 6 may not be needed at all. The
16 compression performed in step 6 (including compression by 50% or
17 more) can be performed by any suitable technique, including one,
18 or a combination of, the following techniques: advanced matrix
19 arithmetic compression, vector based compression, quantum
20 compression, sliding window compression, or key folding using bit
21 swapping. The compression can be applied to individual bits,
22 whole bytes, or partial bytes.
23
24

25 The compression technique that will now be described is key
26 folding using bit swapping. This technique is accomplished by
27 discarding the four MSB of each byte in T, and using these
28

vacated positions to temporarily store the four LSB from half of the bytes of T. In the example illustrated above, the four MSB of the ASCII values 64 (decimal) through 79 (decimal) are 0100 for each byte in T, as can be seen from Table 1. These bits are discarded during folding, and reassembled later (in step 10) upon receipt by party B to recreate the original form of T. Table 2 illustrates key folding using bit swapping, as follows:

T (transport key before folding)

FT (folded transport key)

	MSB	LSB		MSB	LSB
byte 1	0100	0011		0011	1001
byte 2	0100	1001		0101	1101
byte 3	0100	0101			
byte 4	0100	1101			

TABLE 2

It can be seen from the above example that the four LSB in byte 1 of T have been shifted to become the four MSB in byte 1 of FT, the four LSB in byte 2 of T are now the four LSB in byte 1 of FT, the four LSB in byte 3 of T are now the four MSB of byte 2 of FT, and the four LSB of byte 4 of T are now the four LSB in byte 2 of FT.

After folding, the folded transport key FT is 50% of its original size, because each folded byte in FT contains the information from two of the original bytes of T.

1 In step 7, for an OTP cipher system, an exclusive OR (XOR)
2 is performed between the random converted transport key KT from
3 the previous iteration of the method and a new (for that
4 iteration) key set comprising a communications key C and a
5 compressed transport key FT. The result of step 7 is
6 transmittable ciphertext comprising an encrypted communications
7 key EC plus an encrypted compressed transport key EFT.

9 For an OTP cipher system, the encryption performed in step 7
10 must be true OTP encryption, to preserve security. If the
11 communications key C is a key for a weaker non-OTP cryptosystem,
12 this requirement can be relaxed -- the encryption in step 7 does
13 not have to be OTP encryption, and XORing does not have to be
14 used.

16 Step 8 is the distribution of EC and EFT from party A to
17 party B via network 3.

18 While the first eight steps were performed by party A, steps
19 9 and 10 are performed by party B. At step 9, party B decrypts
20 EC and EFT using KT from the previous iteration. The decryption
21 key used in step 9 must be the same as the encryption key used in
22 step 7 for that iteration, and the decryption algorithm must be
23 consistent with the encryption algorithm. The result of step 9
24 is C plus FT.

26 In step 10, FT is uncompressed (unfolded in the illustrated
27 embodiment). The unfolding process is exactly the reverse of the

1 folding process described in step 6 above. Thus, for the
2 illustrated method of key folding by bit swapping, FT is unfolded
3 by splitting each byte of FT into two new bytes, moving the four
4 MSB of each old FT byte into four LSB of a new T byte, and
5 padding 0100 into the four MSB for each new T byte. It is
6 assumed that party B doing the unfolding in step 10 knows the
7 folding range and folding algorithm used by party A in step 6.
8

9 In the method illustrated in Figure 1, transport key T sizes
10 remain uniform, because 50% compression is achieved. Thus, key C
11 upgrades can be performed to infinity, i.e., there can be an
12 infinite number of iterations, even in an OTP cipher system.
13 Throughout, the encryption is secure, because fresh
14 communications keys C and transport keys T are being created for
15 each iteration. If less than 50% compression is achieved in step
16 6, each successive iteration's communications key C will have a
17 smaller and smaller size in many cipher systems, including the
18 OTP cipher system, until the size of the communications key C
19 becomes zero. Thus, the number of iterations is finite when less
20 than 50% compression is utilized in these cipher systems.
21

22 The transport key T retrieved by party B is stored in a
23 secure area within the purview of party B, awaiting the next
24 iteration of the method.
25

26 The communications key C retrieved by party B is placed into
27 service. This can entail using C for encrypted communications
28

1 between party A and party B, or using C to communicate in a
2 secure fashion with a third party. In the case of a One-Time Pad
3 cipher system, the communications key C must be used just once if
4 security is to be preserved. However, portions of a
5 communications key C can be used for one communication, then
6 subsequent portions of key C can be used for subsequent
7 communications. Thus, party B can use a portion of a newly
8 distributed communications key C to communicate with party A and
9 another portion of the newly distributed communications key C to
10 communicate with a third party.

12 When C expires or is about to expire, party B can
13 communicate to party A that it is time for a new iteration of the
14 method to take place, so that party B can receive a new
15 communications key C. This message from party B to party A can
16 be done automatically, and can be done via computer means, e.g.,
17 over network 3. In one embodiment, a monitoring device monitors
18 the degree to which a given communications key C is being
19 exhausted. This information can be displayed in graphical form
20 to party B via a graphical user interface (GUI).

22 The repetition of the method steps can be terminated after a
23 preselected event has occurred. For example, the method can be
24 aborted every week, at which time the method is reinitialized.
25 This may be done to enhance security.

1 The above description is included to illustrate the
2 operation of the preferred embodiments and is not meant to limit
3 the scope of the invention. The scope of the invention is to be
4 limited only by the following claims. From the above discussion,
5 many variations will be apparent to one skilled in the art that
6 would yet be encompassed by the spirit and scope of the present
7 invention. For example, the present invention can be implemented
8 in 16-bit words, 32-bit words, etc.
9

10 What is claimed is:
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28